

AMENDMENT

Amendments to the Claims: Please replace all prior versions and listings of claims with the following listing of claims.

LISTING OF CLAIMS:

1. (Currently Amended) A computer-implemented system for providing service level management ~~in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the system comprising:~~

a network having a plurality of network components that support a service provided over the network, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

a plurality of multiple monitoring agents that each configured to monitor [(a)] respective individual domains aspect of the network that include respective subsets operation of one or more of the plurality of network components that support the service, wherein each the plurality of monitoring agents include:

a first monitoring agent configured to monitor one or more component parameters for a first subset of the plurality of network components in a first domain of the network, detect one or more detects intra-domain events in the first domain as a function of the component parameters respective monitored in the first domain, aspect of operation and generates generate one or more intra-domain alarms in the first domain as a function of the detected intra-domain events detected in the first domain;
and

a second monitoring agent configured to monitor one or more component parameters for a second subset of the plurality of network components in a second domain of the network, detect one or more intra-domain events in the second domain as a function of the component parameters monitored in the second domain, and

generate one or more intra-domain alarms in the second domain as a function of the intra-domain events detected in the second domain; and

an alarm correlation agent configured to:

correlate that receives the intra-domain alarms generated alarms from in the monitoring agents, wherein first domain and the second domain to generate one or more inter-domain alarms across the first domain and the second domain;

map the inter-domain alarms generated across the first domain and the second domain to a service parameter that represents alarm correlation agent determines a current state of the service, wherein the current state of the service is undesirable when based on the received alarms service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issue issues one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service [(is)] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

2. (Currently Amended) The system of claim 1, wherein the plurality of monitoring agents ~~comprise at least one of~~ further include:

at least one [(an)] infrastructure monitoring agent configured to monitor one or more parameters for at least one transmission device in an infrastructure operation of the network infrastructure;

at least one [(a)] computer system monitoring agent configured to monitor one or more parameters for operation of at least one computer system on the network;

at least one a network traffic monitoring agent configured to monitor traffic that flows over transmission media on the infrastructure of the network;

at least one [(an)] application monitoring agent configured to monitor operation of at least one software application operating on the network;

at least one [[a]] trouble-ticketing agent configured to receive reports of problems reported by one or more users with respect to operation of the network;

at least one [[a]] response time ~~monitoring~~ agent configured to monitor [[a]] response time times of a communication one or more communications on the network;

at least one [[a]] device ~~monitoring~~ agent configured to monitor one or more parameters for operation of a an individual device on the network; and

at least one [[a]] multicomponent ~~monitoring~~ agent comprising an aggregate of any of the ~~above monitoring agents~~ infrastructure agent, the system agent, the traffic agent, the application agent, the trouble-ticketing agent, the response time agent, and the device agent.

3. (Currently Amended) The system of claim 1, wherein the plurality of monitoring agents ~~and the alarm correlation agent~~ comprise reasoning agents that provide reactive or reflexive behavior designed for short-term problem solving relating to the service, and wherein the alarm correlation agent comprises a reasoning agent that provides deliberative behavior designed for long-term problem solving relating to the service.

4. (Currently Amended) The system of claim 3, wherein the reasoning agents comprise one or more of:

at least one [[a]] rule-based reasoning agent having a working memory that includes a plurality of facts relating to the service, a rule base that represents knowledge relating to additional facts to infer and actions to take based on the facts in the working memory, and an inference engine configured to make one or more inferences based on the facts in the working memory and the knowledge represented in the rule base;

at least one [[a]] model-based reasoning agent having a plurality of models that represent the plurality of network components that support the service and a correlation architecture that provides collaboration among the plurality of models;

at least one [[a]] state-transition graph based reasoning agent having fuzzy logic that defines grades of membership for a plurality of states, wherein the grades of membership quantify transitions among the plurality of states;

at least one ~~[[a]]~~ code book based reasoning agent; and

at least one ~~[[a]]~~ case-based reasoning agent having a case library that includes a plurality of cases representing episodes of problem solving, a plurality of relevance rules for identifying one or more of the cases in the case library that are relevant to a current problem relating to the service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

5. **(Currently Amended)** The system of claim 1, further comprising~~[[:]]~~ an alarm bucket configured to receive repository~~that receives the generated intra-domain alarms generated in the first domain and the second domain from the first monitoring agents agent and the second monitoring agent,~~ wherein the alarm correlation agent ~~analyzes~~ is further configured to correlate the intra-domain alarms in the alarm repository bucket.

6. **(Currently Amended)** A computer-implemented system for providing service level management in a ~~network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state,~~ the system comprising:

a network having a plurality of network components that support a service provided over the network, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

a first monitoring agent that monitors configured to:

monitor one or more component parameters for a first subset aspect of operation of one or more of the plurality of network components, wherein the in a first domain of the network;

detect one or more intra-domain monitoring agent detects events in the first domain as a function of the component parameters monitored in the first domain; and

generate one or more intra-domain aspect-of-operation-and-generates alarms in the first domain as a function of the detected intra-domain events detected in the first domain;

a second monitoring agent ~~that monitors~~ configured to:

monitor one or more component parameters for a second subset aspect-of operation-of-one-or-more of the plurality of network components, wherein the in a second aspect is different from the first aspect, and wherein domain of the network;

detect one or more intra-domain the-second-monitoring-agent-detects events in the second domain as a function of the component parameters monitored aspect-of operation in the second domain; and

generate one or more intra-domain generates alarms in the second domain as a function of the detected intra-domain events detected in the second domain;

an alarm bucket configured to receive repository-that-receives the generated intra-domain alarms generated in the first domain and the second domain from the first and-second monitoring agents agent and the second monitoring agent; and

an alarm correlation agent ~~that analyzes at least~~ configured to:

correlate the received the intra-domain alarms in the alarm repository, bucket to generate one or more inter-domain alarms across the first domain and the second domain;

map the inter-domain alarms generated across the first domain and the second domain to a service parameter that represents determines a current state of the service based-on-the-analyzed-alarms, wherein the current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issue issues one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service [[is]] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

7-8. (Cancelled)

9. (Currently Amended) The system of claim 6, wherein the first monitoring agent and the second monitoring agents agent comprise at least one of:

at least one [[a]] infrastructure monitoring agent configured to monitor one or more parameters for at least one transmission device in an infrastructure operation of the network infrastructure;

at least one [[a]] computer system monitoring agent configured to monitor one or more parameters for operation of at least one computer system on the network;

at least one a network traffic monitoring agent configured to monitor traffic that flows over transmission media on the infrastructure of the network;

at least one [[a]] application monitoring agent configured to monitor operation of at least one software application operating on the network;

at least one [[a]] trouble-ticketing agent configured to receive reports of problems reported by one or more users with respect to operation of the network;

at least one [[a]] response time monitoring agent configured to monitor [[a]] response time times of a communication one or more communications on the network;

at least one [[a]] device monitoring agent configured to monitor one or more parameters for operation of a an individual device on the network; and

at least one [[a]] multicomponent monitoring agent comprising an aggregate of any of the above monitoring agents infrastructure agent, the system agent, the traffic agent, the application agent, the trouble-ticketing agent, the response time agent, and the device agent.

10. (Currently Amended) The system of claim 6, wherein the first monitoring agent and the second monitoring agents agent comprise reasoning agents that provide reactive or reflexive behavior designed for short-term problem solving relating to the service, and wherein the alarm correlation agent comprise a reasoning agents agent that provides deliberative

behavior designed for long-term problem solving relating to the service, wherein the reasoning agents comprise one or more of:

at least one [[a]] rule-based reasoning agent having a working memory that includes a plurality of facts relating to the service, a rule base that represents knowledge relating to additional facts to infer and actions to take based on the facts in the working memory, and an inference engine configured to make one or more inferences based on the facts in the working memory and the knowledge represented in the rule base;

at least one [[a]] model-based reasoning agent having a plurality of models that represent the plurality of network components that support the service and a correlation architecture that provides collaboration among the plurality of models;

at least one [[a]] state-transition graph based reasoning agent having fuzzy logic that defines grades of membership for a plurality of states, wherein the grades of membership quantify transitions among the plurality of states;

at least one [[a]] code book based reasoning agent; and

at least one [[a]] case-based reasoning agent having a case library that includes a plurality of cases representing episodes of problem solving, a plurality of relevance rules for identifying one or more of the cases in the case library that are relevant to a current problem relating to the service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

11. (Currently Amended) A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components and at least one monitoring agent that monitors an aspect of operation of one or more of the network components, wherein the monitoring agent detects events in the monitored aspect of operation and generates alarms as a function of the detected events, and wherein a service operates on a subset of the plurality of network components, the service having a state, the system comprising:

a network having a plurality of network components that support a service provided over the network, wherein performance of the service depends upon performances of the

plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

a plurality of monitoring agents, wherein each of the plurality of monitoring agents are configured to:

monitor one or more component parameters for a subset of the plurality of network components in a respective domain of a plurality of domains of the network;

detect one or more intra-domain events in the respective domain as a function of the component parameters monitored in the respective domain; and

generate one or more intra-domain alarms in the respective domain as a function of the intra-domain events detected in the respective domain; and

an alarm correlation agent, wherein the alarm correlation agent is that receives configured to:

correlate the generated intra-domain alarms from generated in the monitoring agent, wherein respective domains by the plurality of monitoring agents to generate one or more inter-domain alarms across the plurality of domains of the network;

map the inter-domain alarms generated across the plurality of domains of the network to a service parameter that represents alarm correlation agent determines a current state of the service, wherein based on the received alarms current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issue issues one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service [[is]] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

12. (Currently Amended) The system of claim 11, wherein the alarm correlation agent comprises one or more of a reasoning agent that provides deliberative behavior designed for long-term problem solving relating to the service, wherein the reasoning agent comprises:

at least one [[a]] rule-based reasoning agent having a working memory that includes a plurality of facts relating to the service, a rule base that represents knowledge relating to additional facts to infer and actions to take based on the facts in the working memory, and an inference engine configured to make one or more inferences based on the facts in the working memory and the knowledge represented in the rule base;

at least one [[a]] model-based reasoning agent having a plurality of models that represent the plurality of network components that support the service and a correlation architecture that provides collaboration among the plurality of models;

at least one [[a]] state-transition graph based reasoning agent having fuzzy logic that defines grades of membership for a plurality of states, wherein the grades of membership quantify transitions among the plurality of states;

at least one [[a]] code book based reasoning agent; and

at least one [[a]] case-based reasoning agent having a case library that includes a plurality of cases representing episodes of problem solving, a plurality of relevance rules for identifying one or more of the cases in the case library that are relevant to a current problem relating to the service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

13. **(Currently Amended)** A computer-implemented method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

providing a service over a network having a plurality of network components that support the service, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

monitoring at least one aspect of operation of one or more component parameters for [[of]] the plurality of network components that support the service using a plurality of monitoring agents, wherein each of the plurality of monitoring agents are configured to

monitor a subset of the plurality of network components in a respective domain of a plurality of domains of the network;

detecting one or more intra-domain events in each of the respective domains as a function monitored aspect of operation the component parameters monitored by the plurality of monitoring agents in the respective domains;

generating one or more intra-domain alarms each of the respective domains as a function of the intra-domain detected events detected in the respective domains;

correlating analyzing the generated intra-domain alarms generated in the respective domains using an alarm correlation agent, wherein the alarm correlation agent is configured to determine correlate the intra-domain alarms to generate one or more inter-domain alarms across the plurality of domains of the network;

mapping the inter-domain alarms generated across the plurality of domains of the network to a service parameter that represents a current state of the service, wherein the current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issuing one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service [[is]] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

14. (Cancelled)

15. (Currently Amended) The method according to claim 13, wherein the component parameters monitored by the plurality aspects of monitoring agents in the respective domains operation include at least one of:

one or more parameters for at least one transmission device in an infrastructure operation of the network infrastructure;

one or more parameters for operation of at least one computer system on the network;

traffic that flows over transmission media on the infrastructure of the network;

~~operation of at least one software application operating on the network; and~~
~~operation of a trouble-ticketing agent that receives reports of problems reported by~~
~~one or more users with respect to operation of the network;~~

~~one or more parameters for operation of a an individual device on the network;~~

~~[[a]] response time times of a communication one or more communications on the~~
~~network; and~~

~~an aggregate of any of the above aspects of operation~~ transmission device parameters,
the computer system parameters, the transmission media traffic, the software application, the
reports of problems, the individual device parameters, and the response times.

16. (Currently Amended) The method of claim 13, wherein ~~generating the plurality of~~
~~monitoring agents apply reasoning to detect the intra-domain events and generate the intra-~~
~~domain alarms, wherein the reasoning includes applying at least one of:~~

applying rule-based reasoning using a working memory that includes a plurality of facts
relating to the service, a rule base that represents knowledge relating to additional facts to
infer and actions to take based on the facts in the working memory, and an inference engine
configured to make one or more inferences based on the facts in the working memory and the
knowledge represented in the rule base;

applying model-based reasoning using a plurality of models that represent the plurality
of network components that support the service and a correlation architecture that provides
collaboration among the plurality of models;

applying state-transition graph based reasoning using fuzzy logic that defines grades of
membership for a plurality of states, wherein the grades of membership quantify transitions
among the plurality of states;

applying code book based reasoning; and

applying case-based reasoning using a case library that includes a plurality of cases
representing episodes of problem solving, a plurality of relevance rules for identifying one or
more of the cases in the case library that are relevant to a current problem relating to the

service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

17. (Currently Amended) The method of claim 13, wherein the alarm correlation agent applies reasoning to generate analyzing the generated inter-domain alarms, wherein the reasoning includes applying at least one of:

applying rule-based reasoning using a working memory that includes a plurality of facts relating to the service, a rule base that represents knowledge relating to additional facts to infer and actions to take based on the facts in the working memory, and an inference engine configured to make one or more inferences based on the facts in the working memory and the knowledge represented in the rule base;

applying model-based reasoning using a plurality of models that represent the plurality of network components that support the service and a correlation architecture that provides collaboration among the plurality of models;

applying state-transition graph based reasoning using fuzzy logic that defines grades of membership for a plurality of states, wherein the grades of membership quantify transitions among the plurality of states;

applying code book based reasoning; and

applying case-based reasoning using a case library that includes a plurality of cases representing episodes of problem solving, a plurality of relevance rules for identifying one or more of the cases in the case library that are relevant to a current problem relating to the service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

18. (Currently Amended) A computer-implemented method for providing service level management ~~in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method~~ comprising:

providing a service over a network having a plurality of network components that support the service, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

monitoring one or more component parameters for a first subset aspect of operation of one or more of the plurality of network components in a first domain of the network using a first monitoring agent;

detecting one or more intra-domain events in the first domain as a function monitored aspect of operation the component parameters monitored in the first domain using the first monitoring agent;

generating a first set of one or more intra-domain alarms in the first domain as a function of the detected intra-domain events detected in the first monitored aspect of operation domain using the first monitoring agent;

monitoring one or more component parameters for a second subset aspect of operation of one or more of the plurality of network components, wherein the in a second domain of aspect is different from the first aspect network using a second monitoring agent;

detecting one or more intra-domain events in the second domain as a function monitored aspect of operation the component parameters monitored in the second domain using the second monitoring agent;

generating a second set of one or more intra-domain alarms in the second domain as a function of the detected intra-domain events detected in the second monitored aspect of operation domain using the second monitoring agent;

receiving sending the intra-domain alarms generated in the first domain and the second domain from the first monitoring agent and the second monitoring agent, wherein the intra-domain alarms are received at sets of alarms to an alarm repository bucket;

correlating analyzing at least the intra-domain first and second generated sets of alarms in the alarm repository bucket using an alarm correlation agent, wherein the alarm correlation agent is configured to determine correlate the intra-domain alarms to generate one or more inter-domain alarms across the plurality of domains of the network;

mapping the inter-domain alarms generated across the plurality of domains of the network to a service parameter that represents a current state of the service, wherein the current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issuing one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service ~~[[is]]~~ being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

19. (Cancelled)

20. (Currently Amended) The method of claim 18, wherein the one or more issued instructions control one or more component parameters for an aspect of operation of one or more of the plurality of network components that support the service, wherein the one or more instructions are issued to cause the service parameter value to meet or exceed or the service level identified in the service level agreement.

21. (Currently Amended) A computer readable medium having computer executable instructions recorded thereon, wherein the computer executable instructions are operable to direct a computer to perform a method for providing service level management ~~in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:~~

providing a service over a network having a plurality of network components that support the service, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

monitoring ~~at least one aspect of operation of~~ one or more component parameters for ~~[[of]]~~ the plurality of network and components that support the service using a plurality of

monitoring agents, wherein each of the plurality of monitoring agents are configured to monitor a subset of the plurality of network components in a respective domain of a plurality of domains of the network;

detecting one or more intra-domain events in each of the respective domains as a function monitored aspect of operation the component parameters monitored by the plurality of monitoring agents in the respective domains;

generating one or more intra-domain alarms each of the respective domains as a function of the intra-domain detected events detected in the respective domains;

correlating analyzing the generated intra-domain alarms generated in the respective domains using an alarm correlation agent, wherein the alarm correlation agent is configured to determine correlate the intra-domain alarms to generate one or more inter-domain alarms across the plurality of domains of the network;

mapping the inter-domain alarms generated across the plurality of domains of the network to a service parameter that represents a current state of the service, wherein the current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issuing one or more instructions to autonomously establish a desirable state of the service when in response to the current state of the service [[is]] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

22. (Cancelled)

23. (Currently Amended) A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of components, the service having a state, the system comprising:

a network having a plurality of network components that support a service provided over the network, wherein performance of the service depends upon performances of the

plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

a plurality of ~~multiple~~ monitoring agents ~~that each~~ configured to monitor [(a)]
respective individual domains ~~aspect of the network~~ that include respective subsets ~~operation~~
~~of one or more~~ of the plurality of network components that support the service, wherein each
the plurality of monitoring agents is configured to detect ~~agent detects~~ one or more intra-
domain events in the respective domain as a function of the component parameters monitored
in the respective domain ~~aspect of operation~~ and ~~generates~~ generate one or more intra-
domain alarms in the respective domain as a function of the ~~detected~~ intra-domain events
detected in the respective domain, wherein each of the plurality of monitoring agent including
agents include:

an alarm correlation agent configured to correlate the intra-domain that
~~receives the generated alarms~~ generated in the respective domain in addition to one or
more intra-domain alarms generated in the other individual domains by the other
monitoring agents to generate one or more inter-domain alarms across the individual
domains of the network, wherein ~~map~~ the inter-domain alarms generated across the
individual domains and to a service parameter that represents ~~alarm correlation agent~~
determines a current state of the service, wherein ~~based on the received alarms~~ current
state of the service is undesirable when the service parameter has a value that does not
meet or exceed a service level identified in a service level agreement; and

a control agent configured to control ~~controls~~ the component parameters for
the subset of the plurality of network components in the respective monitored domain
~~aspect of operation, wherein the control agent issues and issue~~ one or more
instructions for one or more of ~~regarding~~ the controlled component parameters ~~aspect~~
~~of operation~~ to autonomously establish a desirable state of the service when in
response to the current state of the service [(is)] being undesirable, wherein the
desirable state of the service is established when the instructions cause the value of the
service parameter to meet or exceed the service level identified in the service level
agreement.

24. (Currently Amended) The system of claim 23, wherein the plurality of monitoring agents ~~comprise at least one of~~ further include:

at least one ~~[[a]]~~ infrastructure ~~monitoring agent configured~~ to monitor one or more parameters for at least one transmission device in an infrastructure operation of the network infrastructure;

at least one ~~[[a]]~~ computer system ~~monitoring agent configured~~ to monitor one or more parameters for operation of at least one computer system on the network;

at least one ~~a network~~ traffic ~~monitoring agent configured~~ to monitor traffic that flows over transmission media on the infrastructure of the network;

at least one ~~[[a]]~~ application ~~monitoring agent configured~~ to monitor ~~operation of~~ at least one software application operating on the network;

at least one ~~[[a]]~~ trouble-ticketing agent ~~configured~~ to receive reports of problems reported by one or more users with respect to operation of the network;

at least one ~~[[a]]~~ response time ~~monitoring agent configured~~ to monitor ~~[[a]] response time times of a communication one or more communications~~ on the network;

at least one ~~[[a]]~~ device ~~monitoring agent configured~~ to monitor one or more parameters for operation of a an individual device on the network; and

at least one ~~[[a]]~~ multicomponent ~~monitoring agent comprising an aggregate of any of the above monitoring agents infrastructure agent, the system agent, the traffic agent, the application agent, the trouble-ticketing agent, the response time agent, and the device agent.~~

25. (Currently Amended) The system of claim 23, wherein the plurality of monitoring agents comprise reasoning agents that provide reactive or reflexive behavior designed for short-term problem solving relating to the service, and wherein the alarm correlation agent within each of the plurality of monitoring agents comprises a reasoning agent that provides deliberative behavior designed for long-term problem solving relating to the service, and wherein the reasoning agents comprise at least one of:

at least one [[a]] rule-based reasoning agent having a working memory that includes a plurality of facts relating to the service, a rule base that represents knowledge relating to additional facts to infer and actions to take based on the facts in the working memory, and an inference engine configured to make one or more inferences based on the facts in the working memory and the knowledge represented in the rule base;

at least one [[a]] model-based reasoning agent having a plurality of models that represent the plurality of network components that support the service and a correlation architecture that provides collaboration among the plurality of models;

at least one [[a]] state-transition graph based reasoning agent having fuzzy logic that defines grades of membership for a plurality of states, wherein the grades of membership quantify transitions among the plurality of states;

at least one [[a]] code book based reasoning agent; and

at least one [[a]] case-based reasoning agent having a case library that includes a plurality of cases representing episodes of problem solving, a plurality of relevance rules for identifying one or more of the cases in the case library that are relevant to a current problem relating to the service, and parameterized adaption logic that adapts solutions variables associated with the identified cases for the current problem relating to the service.

26. (Currently Amended) A computer readable medium having computer executable instructions recorded thereon, wherein the computer executable instructions are operable to direct an agent operating on each of a plurality of agents computer to perform a method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

providing a service over a network having a plurality of network components that support the service, wherein performance of the service depends upon performances of the plurality of network components that support the service, and wherein the service has a state that represents the performance of the service;

monitoring ~~at least one respective aspect of operation~~ a plurality of domains of the network using the agent operating on the computer, wherein the monitored domain includes a subset one or more of the plurality of network and components that support the service;

detecting one or more intra-domain events in the ~~respective~~ monitored domain as a function aspect of operation the component parameters monitored in the domain;

generating one or more intra-domain alarms in the monitored domain as a function of the ~~detected~~ intra-domain events detected in the monitored domain;

communicating with one or more other agents in the other domains of the network to access intra-domain events [or] and intra-domain alarms across the plurality in other ~~respective monitored aspects of operation domains of the network;~~

correlating analyzing at least the generated intra-domain alarms generated in the monitored domain, and the accessed intra-domain events detected across the plurality of domains, and the intra-domain [or] alarms generated across the plurality of domains to generate one or more inter-domain alarms across the plurality of domains of the network;

mapping the inter-domain alarms generated across the plurality of domains to a service parameter that represents ~~determine~~ a current state of the service, wherein the current state of the service is undesirable when the service parameter has a value that does not meet or exceed a service level identified in a service level agreement; and

issuing one or more instructions to autonomously establish a desirable state of the service ~~when in response to~~ the current state of the service [is] being undesirable, wherein the desirable state of the service is established when the instructions cause the value of the service parameter to meet or exceed the service level identified in the service level agreement.

27. (New) The system of claim 1, wherein the service level agreement further identifies one or more penalties for a supplier of the service when the value of the service parameter does not meet or exceed the service level identified in the service level agreement.

28. (New) The system of claim 27, wherein the service level agreement further identifies one or more rewards for the supplier of the service when the value of the service parameter meets or exceeds the service level identified in the service level agreement.